

# BREVET D'INVENTION

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

## COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 25 MARS 2003

**DOCUMENT DE PRIORITÉ**

PRÉSENTÉ OU TRANSMIS  
CONFORMÉMENT À LA  
RÈGLE 17.1.a) OU b)

Pour le Directeur général de l'Institut  
national de la propriété industrielle  
Le Chef du Département des brevets

Martine PLANCHE

INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

SIEGE  
26 bis, rue de Saint Petersburg  
75800 PARIS cedex 08  
Téléphone : 33 (0)1 53 04 53 04  
Télécopie : 33 (0)1 53 04 45 23  
www.inpi.fr



INSTITUT  
NATIONAL DE  
LA PROPRIÉTÉ  
INDUSTRIELLE

15, rue de Saint Pétersbourg

Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

# BREVET D'INVENTION CERTIFICAT D'UTILITÉ

Code de la propriété intellectuelle - Livre VI



N° 11354\*01

## REQUÊTE EN DÉLIVRANCE

page 1/2



Cet imprimé est à remplir lisiblement à l'encre noire

08 540 W / 300301

<b>DES PIÈCES</b>  <b>28 MAI 2002</b> <b>75 INPI PARIS</b> <b>REGISTREMENT</b> <b>N° ATTRIBUÉ PAR L'INPI</b> <b>0206514</b> <b>DATE DÉPÔT ATTRIBUÉE</b> <b>INPI</b> <b>28 MAI 2002</b> <b>Références pour ce dossier</b> <b>(facultatif)</b> <b>BIF114616/FR</b>	<b>NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE</b> <b>À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE</b>  <b>CABINET BONNET-THIRION</b> <b>12, avenue de la Grande Armée,</b> <b>75017 PARIS</b>
---	--


<b>Information d'un dépôt par télécopie</b>	<input type="checkbox"/> N° attribué par l'INPI à la télécopie
<b>NATURE DE LA DEMANDE</b>	<b>Cochez l'une des 4 cases suivantes</b>
Demande de brevet	<input checked="" type="checkbox"/>
Demande de certificat d'utilité	<input type="checkbox"/>
Demande divisionnaire	<input type="checkbox"/>
<i>Demande de brevet initiale</i>	N° _____ Date _____
<i>ou demande de certificat d'utilité initiale</i>	N° _____ Date _____
Transformation d'une demande de brevet européen <i>Demande de brevet initiale</i>	<input type="checkbox"/> N° _____ Date _____

<b>TITRE DE L'INVENTION (200 caractères ou espaces maximum)</b>  <b>Entité électronique transactionnelle sécurisée par mesure du temps.</b>
---

<b>DÉCLARATION DE PRIORITÉ</b> <b>DU REQUÊTE DU BÉNÉFICE DE</b> <b>LA DATE DE DÉPÔT D'UNE</b> <b>DEMANDE ANTÉRIEURE FRANÇAISE</b>	<b>Pays ou organisation</b> <b>FRANCE</b> <b>Date</b> <b>28 05 2002</b> <b>N°</b> <b>0203916</b> <b>Pays ou organisation</b> _____ <b>N°</b> _____ <b>Date</b> _____ <b>N°</b> _____ <b>Pays ou organisation</b> _____ <b>N°</b> _____ <b>Date</b> _____ <b>N°</b> _____ <input type="checkbox"/> <b>S'il y a d'autres priorités, cochez la case et utilisez l'imprimé «Suite»</b>
--	--

<b>DEMANDEUR</b> <b>Nom ou dénomination sociale</b>  <b>Prénoms</b> <b>Forme juridique</b> <b>N° SIREN</b> <b>Code APE-NAF</b>  <b>Adresse</b> <b>Rue</b> <b>Code postal et ville</b> <b>Pays</b>  <b>Nationalité</b> <b>N° de téléphone (facultatif)</b> <b>N° de télécopie (facultatif)</b> <b>Adresse électronique (facultatif)</b>	<input checked="" type="checkbox"/> <b>S'il y a d'autres demandeurs, cochez la case et utilisez l'imprimé «Suite»</b>  <b>OBERTHUR CARD SYSTEMS SA</b>  <b>Société anonyme</b>  <b>102, Boulevard Malesherbes,</b>  <b>75017 PARIS</b>  <b>FRANCE</b> <b>FRANCAISE</b>
--	---

Remplir impérativement la 2<sup>ème</sup> page

REMISE DES PIÈCES DATE <b>28 MAI 2002</b> LIEU <b>75 INPI PARIS</b> N° D'ENREGISTREMENT <b>0206514</b> NATIONAL ATTRIBUÉ PAR L'INPI		Réservé à l'INPI
<b>Vos références pour ce dossier :</b> <i>(facultatif)</i>		<b>BIF114616/FR</b>
<b>6 MANDATAIRE</b> Nom Prénom Cabinet ou Société N° de pouvoir permanent et/ou de lien contractuel Adresse Rue Code postal et ville N° de téléphone <i>(facultatif)</i> N° de télécopie <i>(facultatif)</i> Adresse électronique <i>(facultatif)</i>		<b>CABINET BONNET-THIRION</b>           <b>12 AVENUE DE LA GRANDE ARMÉE</b>  <b>75 017 PARIS</b> <b>01 53 81 17 00</b>
<b>7 INVENTEUR (S)</b> Les inventeurs sont les demandeurs		<input type="checkbox"/> Oui <input checked="" type="checkbox"/> Non <b>Dans ce cas fournir une désignation d'inventeur(s) séparée</b>
<b>8 RAPPORT DE RECHERCHE</b> Établissement immédiat ou établissement différé		Uniquement pour une demande de brevet (y compris division et transformation) <input checked="" type="checkbox"/> Établissement immédiat <input type="checkbox"/> Établissement différé
Paiement échelonné de la redevance		<b>Paiement en deux versements, uniquement pour les personnes physiques</b> <input type="checkbox"/> Oui <input type="checkbox"/> Non
<b>9 RÉDUCTION DU TAUX DES REDEVANCES</b>		Uniquement pour les personnes physiques <input type="checkbox"/> Requête pour la première fois pour cette invention (joindre un avis de non-imposition) <input type="checkbox"/> Requête antérieurement à ce dépôt (joindre une copie de la décision d'admission pour cette invention ou indiquer sa référence) :
Si vous avez utilisé l'imprimé «Suite», indiquez le nombre de pages jointes		
<b>10 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE</b> (Nom et qualité du signataire)  Bruno QUANTIN N°92.1206 CABINET BONNET-THIRION		<b>VISA DE LA PRÉFECTURE OU DE L'INPI</b>  <b>L. GUICHET</b>

L'invention concerne une entité électronique transactionnelle et a notamment pour objet un perfectionnement apporté à une telle entité électronique pour que celle-ci puisse élaborer une indication au moins en partie représentative d'un temps écoulé entre deux évènements, ce perfectionnement étant remarquable par son niveau d'intégration et son fonctionnement autonome, c'est-à-dire indépendant de tout système extérieur de mesure du temps (générateur de signal d'horloge ou analogue) et par conséquent relativement inviolable. A titre d'exemple, l'invention peut s'appliquer à toute entité électronique transactionnelle autonome comme, par exemple, une carte à microcircuit, comportant des moyens lui permettant d'être couplée au moins temporairement à une source d'énergie électrique pour la mise en œuvre d'une transaction. L'invention peut notamment permettre de déterminer le temps qui s'écoule entre deux transactions successives, la connaissance de cette donnée supplémentaire permettant de détecter une tentative de fraude et par conséquent de sécuriser davantage les transactions. Par transaction on entend de façon très générale un quelconque échange de données entre l'entité électronique en question et tout serveur hébergeant un logiciel capable de piloter ladite transaction, à savoir, par exemple, un ordinateur, un automate équipé d'un lecteur de carte à microcircuit, ou tout autre équipement capable d'échanger des informations avec une telle carte à microcircuit ou une entité électronique transactionnelle équivalente. Il est à noter que l'invention est intéressante dans ce contexte, par le fait que les moyens permettant de déterminer le temps qui s'écoule entre deux transactions peuvent se situer dans l'entité électronique transactionnelle autonome et ne nécessitent aucune source d'énergie électrique intégrée à ladite entité.

Le propre d'une transaction sécurisée est de prendre en compte certains paramètres comme, par exemple, l'identité du porteur de l'entité électronique transactionnelle autonome (la carte à microcircuit), la connaissance d'un code connu du porteur, ou encore un intervalle de temps considéré comme normal ou anormal, entre deux évènements. Par exemple, les transactions qui ne contiennent pas une indication du moment où elles ont été effectuées sont

considérées comme beaucoup moins sûres, voire inacceptables dans certains cas. L'invention apporte une solution à ce type de problème.

5 Plus spécifiquement, l'invention concerne une entité électronique transactionnelle caractérisée en ce qu'elle comporte au moins un sous-ensemble comprenant un composant capacitif présentant une fuite au travers de son espace diélectrique, des moyens permettant de coupler ledit composant capacitif à une source d'énergie électrique pour être chargé par ladite source d'énergie électrique et un moyen de mesure de la charge résiduelle dudit composant capacitif, ladite charge résiduelle étant au moins en partie représentative d'un  
10 temps écoulé après que ledit composant capacitif ait été découplé de ladite source d'énergie électrique.

Dans le cas d'une entité électronique autonome, comme par exemple une carte à microcircuit, l'entité électronique dans son ensemble comporte des moyens lui permettant d'être couplée à une source d'énergie électrique et, dans  
15 ce cas, ledit composant capacitif du sous-ensemble ne peut être chargé que lorsque l'entité électronique est couplée à la source d'énergie électrique. Celle-ci est extérieure à l'entité. Par exemple, l'entité électronique pourra être pourvue d'un moyen de commutation pour découpler ledit composant capacitif de la source d'énergie électrique, cet événement initialisant la mesure du temps. Plus  
20 généralement, la mesure du temps, c'est-à-dire la variation de charge du composant capacitif commence dès lors que, après avoir été chargé, celui-ci se trouve électriquement isolé de tout autre circuit et ne peut plus se décharger qu'à travers son propre espace diélectrique.

Cependant, même si physiquement la charge résiduelle mesurée est liée  
25 à l'intervalle de temps écoulé entre l'isolement de l'élément capacitif et une mesure donnée de sa charge résiduelle, un intervalle de temps mesuré (qui sera considéré comme normal ou anormal ou qui pourra de toute façon être pris en compte pour déterminer si l'utilisation qui est faite de l'entité électronique est normale ou anormale) peut être déterminé entre deux mesures, la première  
30 mesure déterminant en quelque sorte une charge résiduelle de référence. Le moyen de mesure est mis en œuvre lorsqu'on désire connaître un temps écoulé.

Par exemple, la sécurité d'une transaction peut être améliorée s'il est possible de prendre en compte le temps qui s'est écoulé entre deux transactions

mettant en œuvre la même entité électronique autonome, par exemple une carte à microcircuit telle qu'une carte bancaire ou une carte de contrôle d'accès ou autre.

5 Ainsi, si l'instant auquel la transaction s'est effectuée peut être mémorisé par un serveur ou un système central et si l'entité autonome est capable d'évaluer le temps qui s'écoule entre deux transactions, la comparaison de ces données peut permettre d'augmenter la sécurité de la transaction, c'est-à-dire de détecter une tentative de fraude qui ne pourrait prendre en compte la connaissance de ces paramètres.

10 Or, la plupart des cartes à microcircuit ne peuvent vérifier l'information relative au temps, qui pourrait leur être fournie lors d'une transaction, pour la simple raison qu'elles ne disposent pas d'horloge interne capable de fonctionner lorsqu'elles sont hors tension. Ce problème trouve un début de solution si la carte à microcircuit est équipée d'un accumulateur électrique, sous forme de film,  
15 logé dans l'épaisseur de la carte en matière plastique. Cette solution est cependant coûteuse, fragile compte tenu de sa construction, mais aussi vulnérable puisqu'un fraudeur peut facilement avoir accès à la source d'énergie et par conséquent aux valeurs du courant qui est, comme on sait, l'un des moyens classiques (connu sous l'appellation DPA pour Differential Power  
20 Analysis, en anglais) permettant de casser un processus cryptographique.

L'invention permet à une telle entité de donner une information sur le temps qui sépare deux transactions tout en assurant la validité de cette information. L'idée de base de l'invention consiste à mesurer le temps entre deux transactions par des moyens qui ne nécessitent pas d'avoir recours à une  
25 alimentation électrique interne.

Plus précisément, l'invention concerne une entité électronique transactionnelle autonome comportant des moyens lui permettant d'être couplée à une source d'énergie électrique extérieure, pour mise en œuvre d'une transaction, caractérisée en ce qu'elle comporte au moins un sous-ensemble  
30 comprenant un composant capacitif présentant une fuite au travers de son espace diélectrique, connecté pour être chargé par ladite source d'énergie électrique extérieure au cours d'une transaction et un moyen de mesure de la

charge résiduelle dudit composant capacitif, ladite charge résiduelle étant au moins en partie représentative du temps écoulé depuis la dernière transaction.

Selon un mode de réalisation préféré, le moyen de mesure comprend un transistor à effet de champ dont la grille est connectée à une borne dudit composant capacitif, c'est-à-dire à une "armature" d'une capacité. Une telle capacité peut être réalisée en technologie MOS dont l'espace diélectrique est constitué par un oxyde de silicium. Dans ce cas, il est avantageux que le transistor à effet de champ soit réalisé également en technologie MOS. La grille du transistor à effet de champ et l'"armature" du composant capacitif MOS sont reliées et constituent une sorte de grille flottante qui peut être connectée à un composant permettant d'injecter des porteurs de charge. On peut aussi faire en sorte qu'il n'existe aucune connexion électrique à proprement parler avec l'environnement extérieur. La connexion de la grille flottante peut être remplacée par une grille de contrôle (électriquement isolée) qui vient charger la grille flottante, par exemple par effet tunnel ou par "porteurs chauds". Cette grille permet de faire transiter des porteurs de charge vers la grille flottante commune au transistor à effet de champ et au composant capacitif. Cette technique est bien connue des fabricants de mémoires de type EPROM ou EEPROM. La grille commune flottante reste isolée pendant le temps qui s'écoule entre deux connexions ou couplages à une source d'énergie extérieure, c'est-à-dire à l'occasion de deux transactions successives. Le transistor et le composant capacitif peuvent alors constituer une unité intégrée au microcircuit ou faisant partie d'un autre microcircuit logé dans la même entité autonome.

Pendant une transaction, lorsque l'entité électronique autonome est encore couplée à une source d'énergie électrique extérieure, le composant capacitif est chargé à une valeur prédéterminée, connue ou mesurée et mémorisée, et le moyen de mesure est relié à une borne de ce composant capacitif. A la fin de la transaction, le moyen de mesure, notamment le transistor à effet de champ, n'est plus alimenté mais sa grille reliée à la borne du composant capacitif est portée à une tension correspondant à la charge de celui-ci. Pendant toute la période de temps qui sépare deux transactions, le composant capacitif se décharge lentement au travers de son propre espace diélectrique de sorte que la tension appliquée sur la grille du transistor à effet de

champ diminue progressivement. Au moment où l'entité électronique est à nouveau connectée à une source d'énergie électrique pour la mise en œuvre d'une nouvelle transaction, une tension électrique est appliquée entre le drain et la source du transistor à effet de champ. Ainsi, un courant électrique allant du drain vers la source (ou dans le sens contraire selon les cas) est engendré et peut être recueilli et analysé. La valeur du courant électrique mesuré dépend des paramètres technologiques du transistor à effet de champ et de la différence de potentiel entre le drain et la source, mais aussi de la tension entre la grille et le substrat. Le courant dépend donc des porteurs de charge accumulés dans la grille flottante commune au transistor à effet de champ et au composant capacitif. Par conséquent, ce courant de drain est aussi représentatif du temps qui s'est écoulé entre les deux transactions.

Le courant de fuite d'une telle capacité dépend bien sûr de l'épaisseur de son espace diélectrique mais également de tout autre paramètre dit technologique tel que les longueurs et surfaces de contact des éléments du composant capacitif. Il faut également prendre en compte l'architecture tridimensionnelle des contacts de ces parties qui peuvent induire des phénomènes ayant comme particularité de modifier les paramètres du courant de fuite (par exemple la modification de la valeur de la capacité dite tunnel). Le type et la quantité des dopants et des défauts peuvent être modulés pour modifier les caractéristiques du courant de fuite. Les variations de température ont aussi une influence, plus précisément la moyenne des apports d'énergie calorifique appliqués à la carte entre deux transactions, c'est-à-dire pendant le temps qu'on cherche à déterminer. En fait, tout paramètre intrinsèque à la technologie MOS peut être source de modulation du processus de la mesure du temps. En ce qui concerne les apports calorifiques, cependant, si le diélectrique est d'épaisseur très faible (inférieure à 5 nanomètres), le sous-ensemble correspondant est pratiquement insensible à la température mais la fuite, relativement importante, est telle qu'on ne peut mesurer que des périodes de temps relativement faibles, de l'ordre de quelques minutes ou moins. Un tel sous-ensemble à fuite élevée indépendante de la température, peut cependant être retenu pour la détection de certains types de fraude. Par exemple, ce type de composant capacitif peut permettre de détecter des remises à zéro



successives très rapprochées dans le temps qui sont caractéristiques de certaines attaques dites DPA mentionnées ci-dessus.

Pour mesurer des temps plus longs, il est nécessaire d'utiliser un composant capacitif ayant un espace diélectrique d'épaisseur plus importante. Dans ce cas, la fuite est sensible aux variations de température. Pour obtenir une information sensiblement uniquement représentative du temps, on prévoit au moins deux sous-ensembles tels que définis ci-dessus, exploités "en parallèle". Les deux composants capacitifs sensibles à la température sont définis avec des fuites différentes, toutes choses égales par ailleurs, c'est-à-dire que leurs espaces diélectriques (épaisseur de la couche d'oxyde de silicium) ont des épaisseurs différentes.

A cet effet, selon une disposition avantageuse de l'invention, l'entité électronique définie ci-dessus est caractérisée en ce qu'elle comporte au moins deux sous-ensembles précités comprenant des composants capacitifs présentant des fuites différentes au travers de leurs espaces diélectriques respectifs et en ce qu'elle comporte en outre des moyens de traitement des mesures des charges résiduelles respectives pour extraire desdites mesures une information sensiblement indépendante des apports calorifiques appliqués à ladite entité pendant le temps écoulé entre deux transactions précitées.

Par exemple, les moyens de traitement peuvent comporter un tableau de valeurs de temps mémorisées, ledit tableau étant adressé par lesdites mesures respectives. Autrement dit, chaque couple de mesures désigne une valeur de temps mémorisée indépendante de la température et des variations de température pendant la période mesurée. L'entité électronique comporte normalement une mémoire associée au microprocesseur et une partie de cette mémoire peut être utilisée pour mémoriser ledit tableau.

En variante, les moyens de traitement peuvent comporter un logiciel de calcul programmé pour exécuter une fonction prédéterminée permettant de calculer l'information temps, sensiblement indépendante des apports calorifiques, en fonction des deux mesures précitées.

L'invention sera mieux comprise et d'autres avantages de celle-ci apparaîtront plus clairement à la lumière de la description qui va suivre, donnée

uniquement à titre d'exemple et faite en référence aux dessins annexés dans lesquels :

- la figure 1 est un schéma-bloc d'une carte à microcircuit équipée du perfectionnement selon l'invention ;

5        - la figure 2 est un schéma de principe d'un sous-ensemble précité ; et

- la figure 3 est un schéma-bloc d'une variante.

10        On a représenté une entité électronique transactionnelle autonome 11, ici une carte à microcircuit, comportant des moyens 12 lui permettant d'être couplée à une source d'énergie électrique extérieure 16. Dans l'exemple représenté, l'entité comporte des plages de raccordement métalliques susceptibles d'être connectées à une unité formant lecteur de carte. Deux de ces plages de  
15        raccordement 13a, 13b sont réservées à l'alimentation électrique du microcircuit, la source d'énergie électrique étant logée dans le serveur ou dispositif analogue auquel l'entité électronique autonome est momentanément raccordée. Ces  
20        plages de raccordement pourraient être remplacées par une antenne logée dans l'épaisseur de la carte et susceptible de fournir au microcircuit, l'énergie électrique nécessaire à son alimentation tout en assurant la transmission bidirectionnelle de signaux radiofréquence permettant les échanges d'informations. Le microcircuit comprend un microprocesseur 14 classiquement  
25        associé à une mémoire 15.

30        S'agissant de l'invention, l'entité électronique comporte au moins un sous-ensemble 17 (ou est associée à un tel sous-ensemble) chargé de la mesure du temps. Le sous-ensemble 17 qui est représenté plus en détail à la figure 2 est donc logé dans l'entité électronique. Il peut faire partie du microcircuit et être  
25        réalisé dans la même technologie d'intégration que celui-ci. Dans l'exemple, ce sous-ensemble n'est relié à aucune source d'énergie électrique interne. Il ne peut donc être alimenté que lorsque l'entité électronique est effectivement couplée à un serveur ou un lecteur de carte, comportant une telle source d'énergie électrique. Cependant, si l'entité électronique doit être alimentée en  
30        permanence, le sous-ensemble 17 qui est chargé de la mesure du temps peut être alimenté ou non via des moyens de commutation permettant de la coupler à la source d'énergie électrique ou à l'isoler de celle-ci, ces moyens étant par

exemple partie intégrante du microprocesseur 14, ou constitués par des éléments de commutation gérés par lui.

5 Le sous-ensemble 17 comprend un composant capacitif 20 présentant une fuite au travers de son espace diélectrique 24 et un moyen de mesure 22 de la charge résiduelle de ce composant, ladite charge résiduelle étant au moins en partie représentative du temps écoulé après que le composant capacitif ait été déconnecté de la source d'énergie électrique, dans l'exemple entre deux transactions, c'est-à-dire entre deux opérations où la carte à microcircuit est effectivement couplée à un serveur, c'est-à-dire reliée à une source d'énergie  
10 électrique extérieure. Le composant capacitif est chargé par la source d'énergie électrique extérieure au cours d'une transaction, soit par connexion directe, comme dans l'exemple décrit, soit par tout autre moyen qui peut amener à charger la grille. L'effet tunnel est une méthode permettant de charger la grille sans connexion directe. Dans l'exemple, la charge du composant capacitif est  
15 pilotée par le microprocesseur 14.

Dans l'exemple, le composant capacitif est une capacité en technologie MOS. L'espace diélectrique 24 de cette capacité est constitué par une couche d'oxyde de silicium déposée à la surface d'un substrat 26 constituant l'une des armatures du condensateur. Ce substrat est ici connecté à la masse, c'est-à-dire  
20 à l'une des bornes d'alimentation de la source d'énergie électrique extérieure, lorsque celle-ci se trouve raccordée à la carte. L'autre armature du condensateur est un dépôt conducteur 28a appliqué sur l'autre face de la couche d'oxyde de silicium.

Par ailleurs, ledit moyen de mesure comprend essentiellement un  
25 transistor à effet de champ 30, ici réalisé en technologie MOS, comme la capacité, dont la grille est connectée à une borne du composant capacitif. Dans l'exemple, la grille est un dépôt conducteur 28b de même nature que le dépôt conducteur 28a qui constitue l'armature du composant capacitif. Ces deux dépôts sont reliés l'un à l'autre ou n'en constituent qu'un. Une connexion 32  
30 reliée au microprocesseur 14 permet d'appliquer une tension à ces deux dépôts, pendant un court intervalle de temps nécessaire pour charger le composant capacitif. L'application de cette tension est pilotée par le microprocesseur. Plus généralement, la connexion 32 permet de charger l'élément capacitif 20 à un

moment choisi, sous la commande du microprocesseur et c'est à partir du moment où cette connexion de charge est coupée par le microprocesseur (ou lorsque l'entité électronique est découplée dans son ensemble de toute source d'alimentation électrique) que la décharge du composant capacitif au travers de son espace diélectrique commence, cette perte de charge électrique étant représentative du temps écoulé. La mesure du temps implique la mise en conduction momentanée du transistor 30, ce qui suppose la présence d'une source d'énergie électrique appliquée entre drain et source. Le transistor à effet de champ en technologie MOS comporte, outre la grille, un espace diélectrique de grille 34 séparant cette dernière d'un substrat 36 dans lequel sont définies une région de drain 38 et une région de source 39. L'espace diélectrique de grille 34 est constitué par une couche isolante d'oxyde de silicium. La connexion de source 40 appliquée à la région de source est reliée à la masse et au substrat, tandis que la connexion de drain 41 est reliée à un circuit de mesure du courant de drain qui comporte une résistance 45 aux bornes de laquelle sont connectées les deux entrées d'un amplificateur différentiel 46. La tension délivrée à la sortie de cet amplificateur est donc proportionnelle au courant de drain.

La grille 28b est mise en position flottante pendant le temps qui s'écoule entre deux couplages ou connexions à une source d'énergie extérieure, c'est-à-dire à l'occasion de deux transactions successives. Autrement dit, aucune tension n'est appliquée à la grille pendant cet intervalle de temps. En revanche, puisque la grille est connectée à une armature du composant capacitif 20, la tension de grille pendant cet intervalle de temps est égale à une tension qui se développe entre les bornes dudit composant capacitif et qui résulte d'une charge initiale de celui-ci réalisée sous le contrôle du microprocesseur au cours de la dernière transaction réalisée.

L'épaisseur de la couche isolante du transistor est notablement plus grande que celle du composant capacitif. Par exemple, elle est environ trois fois supérieure à celle du composant capacitif. Selon l'application envisagée, l'épaisseur de la couche isolante du composant capacitif est comprise entre 4 et 10 nanomètres, environ. Lorsque le composant capacitif est chargé par la source extérieure et après que la connexion de charge ait été coupée sous la commande du microprocesseur 14, la tension aux bornes du composant

capacitif 20 diminue lentement au fur et à mesure que ce dernier se décharge progressivement au travers de son propre espace diélectrique. La décharge au travers de l'espace diélectrique du transistor à effet de champ est négligeable compte tenu de l'épaisseur de ce dernier.

5 A titre d'exemple, si, pour une épaisseur d'espace diélectrique donnée, on charge la grille et l'armature du composant capacitif à 6 volts à l'instant  $t = 0$ , le temps associé à une perte de charge de 1 volt, c'est-à-dire un abaissement de la tension à une valeur de 5 volts, est de l'ordre de 24 secondes pour une épaisseur de 8 nanomètres.

10 Pour des épaisseurs différentes, on peut dresser le tableau suivant :

Durée	1 heure	1 journée	1 semaine	1 mois
Epaisseur d'oxyde	8,17 nm	8,79 nm	9,17 nm	9.43 nm
Précision sur le temps	1,85 %	2,09 %	2,24 %	3,10 %

La précision dépend de l'erreur commise sur la lecture du courant de drain (0,1 % environ). Ainsi, pour pouvoir mesurer des temps de l'ordre d'une semaine, on peut prévoir une couche d'espace diélectrique de l'ordre de 9 nanomètres.

15 La figure 2 montre une architecture particulière qui utilise une connexion directe à la grille flottante (28a, 28b) pour y appliquer un potentiel électrique et donc y faire transiter des charges. On peut aussi procéder à une charge indirecte, comme mentionné précédemment, grâce à une grille de contrôle remplaçant la connexion directe, selon la technologie utilisée pour la fabrication des cellules EPROM ou EEPROM.

20 La variante de la figure 3 prévoit trois sous-ensembles 17A, 17B, 17C, chacun associé au microprocesseur 14. Les sous-ensembles 17A et 17B comprennent des composants capacitifs présentant des fuites relativement faibles pour permettre des mesures de temps relativement long. Cependant, ces composants capacitifs sont sensibles aux variations de température, comme  
25 indiqué ci-dessus. Le troisième sous-ensemble 17C comporte un composant capacitif présentant un espace diélectrique très faible, inférieur à 5 nanomètres. Il est de ce fait insensible aux variations de température. Les deux composants capacitifs des sous-ensembles 17A, 17B présentent des fuites différentes au

travers de leurs espaces diélectriques respectifs. En outre, l'entité électrique autonome comporte des moyens de traitement des mesures des charges résiduelles respectives présentes dans les composants capacitifs des deux premiers sous-ensembles 17A, 17B, ces moyens de traitement étant agencés pour extraire desdites mesures une information représentative des temps et sensiblement indépendante des apports calorifiques appliqués à ladite entité pendant le temps écoulé entre deux transactions successives précitées. Dans l'exemple, ces moyens de traitement se confondent avec le microprocesseur 14 et la mémoire 15. En particulier, un espace de cette dernière est réservé à la mémorisation d'un tableau T à double entrée de valeurs de temps et ce tableau est adressé par les deux mesures respectives. Autrement dit, une partie de la mémoire comporte un ensemble de valeurs de temps et chaque valeur correspond à un couple de mesures résultant de la lecture du courant de drain de chacun des deux transistors des sous-ensembles 17A, 17B sensibles à la température.

Ainsi, pendant une transaction, par exemple vers la fin de celle-ci, les deux composants capacitifs sont chargés, à une valeur de tension prédéterminée par la source d'énergie électrique extérieure, via le microprocesseur 14. Lorsque la carte à microcircuit est découplée du serveur ou lecteur de carte, les deux composants capacitifs restent chargés mais commencent à se décharger au travers de leurs propres espaces diélectriques respectifs et, au fur et à mesure que le temps s'écoule, sans que la carte à microcircuit soit utilisée, la charge résiduelle de chacun des composants capacitifs décroît mais différemment dans l'un ou l'autre, en raison des fuites différentes déterminées par construction.

Lorsque la carte est à nouveau couplée à une source d'énergie électrique à l'occasion d'une nouvelle transaction, les charges résiduelles des deux composants capacitifs sont représentatives du même intervalle de temps que l'on cherche à déterminer mais différent en raison des variations de température qui ont pu se produire pendant toute cette période de temps. Au moment de la réutilisation de la carte, les deux transistors à effet de champ de ces deux sous-ensembles sont alimentés et les valeurs des courants de drain sont lues et traitées par le microcircuit. Pour chaque couple de valeurs de courant de drain,

le microcircuit va chercher en mémoire, dans ledit tableau, la valeur de temps correspondante. Cette valeur de temps est ensuite comparée avec la valeur disponible dans le serveur et la transaction n'est autorisée que si ces deux valeurs coïncident ou sont relativement proches.

5           Il n'est pas nécessaire de mémoriser le tableau T. Par exemple, les moyens de traitement, c'est-à-dire essentiellement le microprocesseur 14, peuvent comporter une partie de logiciel de calcul d'une fonction prédéterminée permettant de déterminer ladite information sensiblement indépendante des apports calorifiques en fonction des deux mesures.

10           Le troisième sous-ensemble 17C comporte, comme on l'a vu, un espace diélectrique extrêmement mince le rendant insensible aux variations de température. Ce sous-ensemble peut être utilisé, sous le contrôle du microprocesseur 14, pour détecter des remises à zéro répétées qui se produisent souvent lors d'une attaque de type DPA.

15           D'autres variantes sont possibles. Notamment si on veut simplifier le sous-ensemble 17, on peut envisager de supprimer le composant capacitif 20 en tant que tel car le transistor à effet de champ 30 peut lui-même être considéré comme un composant capacitif avec la grille 28b et le substrat 36 en tant qu'armatures, ces dernières étant séparées par l'espace diélectrique 34. Dans ce

20           cas, on peut considérer que ledit composant capacitif et ledit moyen de mesure sont confondus.

## REVENDEICATIONS

1. Entité électronique transactionnelle caractérisée en ce qu'elle comporte  
5 au moins un sous-ensemble (17) comprenant un composant capacitif (20)  
présentant une fuite au travers de son espace diélectrique, des moyens  
permettant de coupler ledit composant capacitif à une source d'énergie  
électrique pour être chargé par ladite source d'énergie électrique et un moyen de  
10 mesure (22) de la charge résiduelle dudit composant capacitif, ladite charge  
résiduelle étant au moins en partie représentative d'un temps écoulé après que  
ledit composant capacitif ait été découplé de ladite source d'énergie électrique.

2. Entité électronique selon la revendication 1, caractérisée en ce qu'elle  
comporte un moyen de commutation pour découpler ledit composant capacitif de  
ladite source d'énergie électrique.

15 3. Entité électronique selon la revendication 1 ou 2, caractérisée en ce  
que ledit moyen de mesure est mis en œuvre lorsqu'on désire connaître un  
temps écoulé.

4. Entité électronique selon la revendication 1, caractérisée en ce qu'elle  
est autonome et en ce que ladite source d'énergie électrique lui est extérieure.

20 5. Entité électronique selon la revendication 3, caractérisée en ce que  
ledit composant capacitif étant chargé au cours d'une transaction, ledit moyen de  
mesure est mis en œuvre au cours d'une telle transaction pour fournir une  
information au moins en partie représentative du temps écoulé depuis la  
dernière transaction.

25 6. Entité électronique selon l'une des revendications précédentes,  
caractérisée en ce que ledit moyen de mesure comprend un transistor à effet de  
champ (30) dont la grille est connectée à une borne dudit composant capacitif.

7. Entité électronique selon l'une des revendications précédentes,  
caractérisée en ce que ledit composant capacitif (20) est une capacité en  
30 technologie MOS dont l'espace diélectrique est constitué par un oxyde de  
silicium.

8. Entité électronique selon la revendication 6 ou 7, caractérisée en ce  
que ledit transistor à effet de champ est réalisé en technologie MOS, ladite grille



(28b) étant mise en position flottante pendant le temps qui s'écoule entre deux connexions ou couplages à une source d'énergie extérieure, à l'occasion de deux transactions successives.

5 9. Entité électronique selon l'ensemble des revendications 7 et 8, caractérisée en ce que ledit transistor à effet de champ comporte une couche isolante entre l'électrode de grille et un substrat, en ce que ledit composant capacitif comporte une couche isolante (24) formant l'espace diélectrique précité disposé entre une armature (28a) et un substrat (26), et en ce que ladite armature et ladite électrode de grille sont interconnectées.

10 10. Entité électronique selon la revendication 9, caractérisée en ce que l'épaisseur de la couche isolante (34) dudit transistor est notablement plus grande que celle (24) dudit composant capacitif.

15 11. Entité électronique selon la revendication 10, caractérisée en ce que l'épaisseur de ladite couche isolante dudit transistor est environ trois fois supérieure à celle dudit composant capacitif.

12. Entité électronique selon la revendication 10, caractérisée en ce que l'épaisseur de la couche isolante dudit composant capacitif est comprise entre 4 et 10 nanomètres.

20 13. Entité électronique selon l'une des revendications 5 à 12, caractérisée en ce qu'elle comporte au moins deux sous-ensembles (17A, 17B) précités comprenant des composants capacitifs présentant des fuites différentes au travers de leurs espaces diélectriques respectifs et en ce qu'elle comporte en outre des moyens de traitement (14, 15, T) des mesures des charges résiduelles respectives pour extraire desdites mesures une information sensiblement  
25 indépendante des apports calorifiques appliqués à ladite entité pendant le temps écoulé entre deux transactions précitées.

14. Entité électronique selon la revendication 13, caractérisée en ce que lesdits moyens de traitement comportent un tableau de valeurs de temps (T) mémorisées, adressé par lesdites mesures respectives.

30 15. Entité électronique selon la revendication 14, caractérisée en ce qu'elle comporte un espace mémoire définissant ledit tableau.

16. Entité électronique selon la revendication 13, caractérisée en ce que lesdits moyens de traitement comportent un logiciel de calcul d'une fonction

prédéterminée pour déterminer ladite information sensiblement indépendante des apports calorifiques en fonction desdites mesures.

17. Entité électronique selon l'une des revendications précédentes, caractérisée en ce qu'il s'agit d'une carte à microcircuit.

FIG. 1

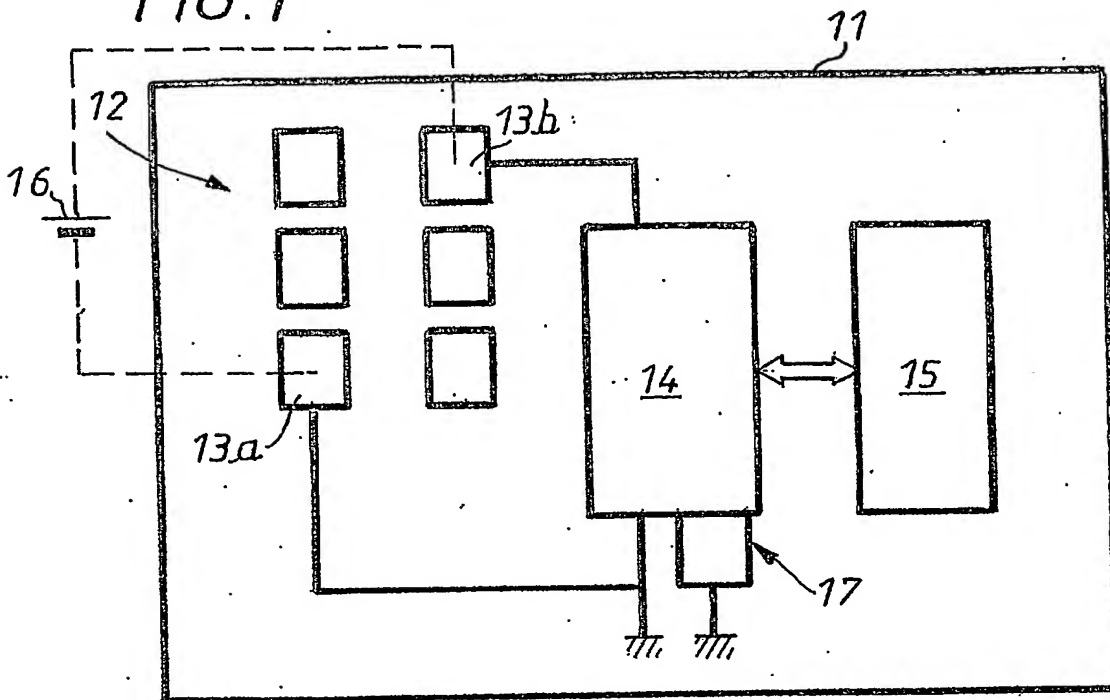


FIG. 2

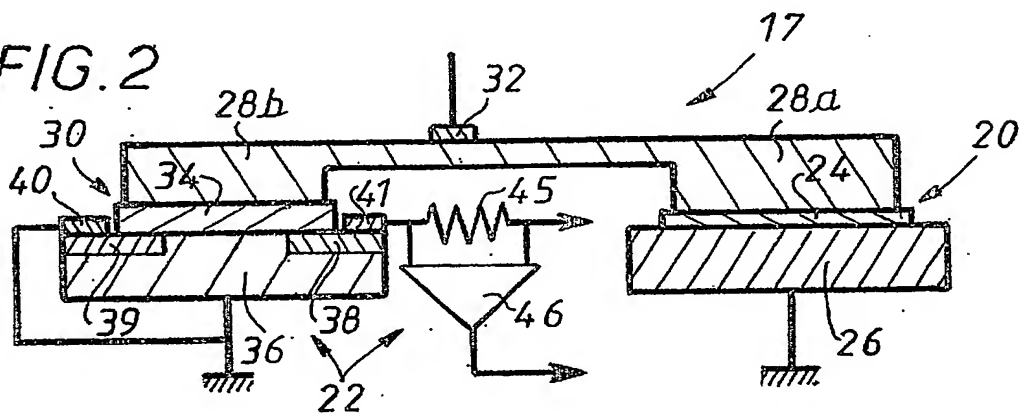
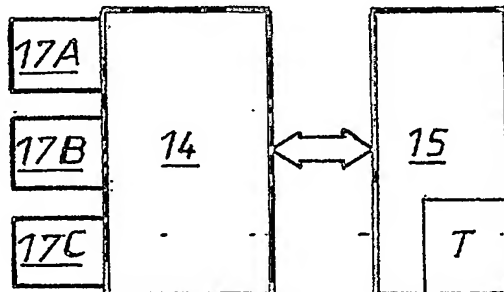


FIG. 3



DÉPARTEMENT DES BREVETS

26 bis, rue de Saint Pétersbourg  
75800 Paris Cedex 08

Téléphone : 33 (1) 53 04 53 04 Télécopie : 33 (1) 42 94 86 54

**DÉSIGNATION D'INVENTEUR(S)** Page N° **1/1**

(Si le demandeur n'est pas l'inventeur ou l'unique inventeur)



Cet imprimé est à remplir lisiblement à l'encre noire

08 113 W / 300301

Vos références pour ce dossier (facultatif)		BIF114616/FR
N° D'ENREGISTREMENT NATIONAL		0206514
TITRE DE L'INVENTION (200 caractères ou espaces maximum)		
Entité électronique transactionnelle sécurisée par mesure du temps.		
LE(S) DEMANDEUR(S) :		
OBERTHUR CARD SYSTEMS SA		
DESIGNE(NT) EN TANT QU'INVENTEUR(S) : (Indiquez en haut à droite «Page N° 1/1» S'il y a plus de trois inventeurs, utilisez un formulaire identique et numérotez chaque page en indiquant le nombre total de pages).		
Nom		SUREAUD
Prénoms		Jean
Adresse	Rue	3646, route de St Jeannet, CD 118
	Code postal et ville	06700 SAINT LAURENT DU VAR
Société d'appartenance (facultatif)		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		
Nom		
Prénoms		
Adresse	Rue	
	Code postal et ville	
Société d'appartenance (facultatif)		
DATE ET SIGNATURE(S) DU (DES) DEMANDEUR(S) OU DU MANDATAIRE (Nom et qualité du signataire)		Le 28 Mai 2002 Bruno QUANTIN N°92.1206 CABINET BONNET-THIRION